FRAUD ON THE INTERNET

A mini-lesson for:

secondary school teachers
adult and community educators
students and consumers

This mini-lesson includes learning objectives, background information, discussion questions, an activity and sources of information.

OBJECTIVES

Learners will:

- identify and describe examples of Internet fraud
- list ways to protect yourself from Internet fraud

Swindlers Have Computers Too

Cyberspace is a vast new territory for unscrupulous marketers. The National Fraud Information Center reports that while fraudulent commercial activity on the Internet is not yet a major problem, as use expands, there is sure to be a major increase in deceptive and misleading promotions.

Swindlers are attracted to the Internet because they can reach thousands of consumers inexpensively, quickly and anonymously. Few restrictions exist on the Internet, making it easy to place deceptive or misleading information online.

Judging the accuracy and reliability of online information is a major challenge for consumers. False or misleading information related to personal finance or health issues, for example, could lead to serious consequences for unsuspecting consumers.

Fraud on the NET

The Federal Trade Commission began investigating fraud on the Internet in 1994. They found that the same kinds of fraud that occur in other places also surface on the Net. Electronic bulletin boards, chat groups and e-mail networks are fertile grounds for old-fashioned scams that apply false advertising claims and deceptive marketing practices.

Electronic Bulletin Boards provide new sources of information to Internet users telling about products, services and investment opportunities. At the same time these electronic bulletin boards can carry false and misleading ads for products that promise quick solutions to desirable goals such as weight loss or easy business success. The plan is to have you use your PC to make plenty of money in a short period of time.

Discussion groups or chat forums often form on the Internet where interested parties can exchange information on specific topic areas. These chat rooms sometimes appear to be open discussion when they are sales pitches in disguise. In some cases, people involved in the discussion may have financial ties to businesses that sell products or services related to the topic area. This disguised advertising may not be obvious to the consumer.

E-mail scams involve individuals or companies intentionally misleading consumers or using deceptive marketing practices to gain the consumer's interest in their product. For example, the use of a particular product is advertised to cure a specific medical condition. These are the same health, diet and fitness schemes that occur in other marketplace venues, such as mail-order, and telemarketing schemes. Other types of e-mail scams involve the sale of worthless products, phony credit repair companies, term paper peddlers, expensive work-at-home deals, psychic hotlines, and deceptive promises related to contests, awards, sweepstakes and free gifts.

Pyramid or Ponzi schemes and chain letters are well suited to the Internet because they entice investors with the promise of quick profits using a home computer. Investors make money by recruiting new investors. The problem is that soon the program runs out of new investors and most players lose the money they invested. Chain letter schemes ask participants to send money to the names at the top of a list with the promise that they will eventually receive thousands of dollars when their names come to the top. Unsuspecting persons lose money every day on this illegal practice.

Risk-free investment opportunities on the Internet offer fraudulent technological and exotic investments such as wireless cable, bogus securities, or worthless land. These investments promise to yield far greater returns than do commonly available investment products. The term "risk-free" is highly misleading. Few consumers get their money back, much less make a profit.

Pump and Dump stock manipulations on the Internet encourage investors to buy a particular stock, which is usually little known and low cost. The promoters may even advertise that they have inside information. They make their profit when consumers buy the stock, or pump up the price and the promoters then promptly sell, or dump their shares and the stock prices immediately fall. This scheme can also work in reverse; a short seller makes a profit when the price of the stock goes down.

Problems With Internet Transactions

Two problems with Internet sales transactions are personal data privacy and verification that both buyers and sellers are authentic. Many consumers are concerned about the confidentiality of their personal financial information on the Web, and with good reason. When you make a purchase on the Internet, your credit card number could fall into the

wrong hands. Personal data can be collected and organized into database files. When you become a part of an on-line service, your personal data can be available to everyone in that system. While it is unlikely that reputable merchants would deliberately sell your data to others, their database may be tempting targets for hackers.

Verification that consumers are who they say they are can be solved by an electronic equivalent of a signature or a driver's license. A software product currently used by merchants, banks and brokerage houses tells who the user is and what privileges he or she has. There is a growing interest in credit card payment systems that would safeguard credit card purchases on the Net. Encryption software can scramble your personal information so that it can be read only by the sender and the receiver. The problem remains that personal data might still be available to certain employees or hackers.

Experts urge consumers to avoid dealing with Internet sites they are not familiar with, and even when dealing with a well-known business, to call the business directly to verify that the site exists. It continues to be a risky business to give personal information, including their address and phone number, credit card numbers, social security numbers, and bank account numbers on the Internet.

Protection Against Internet Fraud

Most people find it hard to believe that they could become victims of fraud, but one should never underestimate the ingenuity of swindlers who make money by misleading others. State and federal laws and agencies have limited capacity to protect consumers from fraud on the Internet. The savvy consumer must stay alert to the possibility of fraud. The National Fraud Information Center offers the following suggestions for side-stepping fraud on the Internet:

- Never reveal checking account numbers, credit card numbers or other personal financial data at any Web site or online service location -- unless you are sure you know where this information will be directed.

- When you subscribe to an on-line service you may be asked for credit card information. When you enter any interactive service site however, beware of con artists who may ask you to "confirm" your enrollment in the service by disclosing passwords or the credit card account number used to subscribe.

- Use the same common sense you would exercise with any direct or telephone credit card purchase. A flashy professional Internet Web site does not guarantee that the sponsor is legitimate. Know the company with which you plan to do business.

- Report anything you see on the Internet that you suspect might be fraudulent. The National Fraud Information Center toll-free number is 1-800-876-7060. Their mailing address is P.O. Box 65868, Washington, D.C. 20035. Their Web address is http://www.fraud.org.

Your state Office of the Attorney General is empowered to investigate consumer complaints, including Internet complaints, and can give you information about any problems or concerns they have encountered with the business.

The Better Business Bureau can tell you if there have been any complaints or inquiries about a business and how it was resolved. Some online advertisements will have a blue-seal that you can click on to connect to the Better Business Bureau for a report on the advertiser's track record. The online Web site for the BBB is http://www.bbbonline.org.

The Federal Trade Commission enforces several consumer protection laws that are relevant to computer transactions, such as false advertising and consumer credit. Suspicious actions on the WEB, when reported to the National Fraud Information Center, are shared with the Federal Trade Commission and the National Association of Attorneys General. In this way, consumers join with state and federal agencies in actions to curtail fraud on the Internet.

Although many regulations and agencies have been established to protect consumers from fraud, the principle of caveat emptor, let the buyer beware, remains the consumer's best protection. Legal protections are limited, fraudulent activities flourish, and once money is lost in a fraudulent scheme the chances of getting it back are extremely small. Awareness of the possibility of fraud is your first line of defense.

See the Department of Financial Institutions Web Sites on Frauds and Scams:
http://www.dfi.state.in.us/conscredit/CIfraud.htm

DISCUSSION QUESTIONS AND TOPICS

1. Why are unscrupulous sellers attracted to the Internet?

2. What is the major problem for consumers with information on the Internet?

3. How can you check out a business that operates on the Internet?

4. How can you protect your personal data when shopping on the Net?

ACTIVITY

Interview the participants in your class or discussion group. Ask them about the advertising they have seen on the Internet such as:

- overstated claims of product effectiveness or exaggerated claims of potential earnings
- claims of inside information
- exotic or technical investments, such as ostrich farming, energy alternatives, gold mining
- no name or address
- references that cannot be checked out
- gifts, prizes or games that require that you send money in order to win
- only available to a limited number of people
- unsolicited e-mail offering to give or sell you anything

After compiling your list of individuals and companies that may be involved in fraudulent activity, contact the National Fraud Information Center to check and see if they have reports on the businesses as well.

You can reach the National Fraud Information Center at:

P.O. Box 65868
Washington, DC 20035
Telephone: 1-800-876-7060
Fax Number: (202) 835-0767
Internet: http://www.fraud.org

Give students a copy of our Brochure.

SOURCES OF ADDITIONAL INFORMATION

Books

Connecting Kids and the Internet: a handbook for librarians, teachers and parents by Allen C. Benson. New York: Neal-Schuman Publishers.

The Internet For Teachers and School Media Specialists: today's applications, tomorrow's prospects. New York: Neal-Schuman Publishers.

Ripoffs And Frauds, How to Avoid and How to Get Away by E. Thomas Garman.. Dame Publications, 7800 Bissonnet, Suite 415, Houston, TX 77074. $13.95. A comprehensive, well-written source of ripoffs and frauds, covering investment swindles, telemarketing and mail scams, vehicle sales and repairs. There is also information on the various regulations, laws, agencies and organizations that can help consumers with fraud.

Articles

Cyberspace 101, Consumer Reports Magazine, pp. 12-17, (May 1996).

Digital Dollars, Mannes, George, Popular Mechanics, pp. 53-103, (January 1996).

Gold Rush in Cyberspace, in Business & Technology section, U.S. News & World Report, pp. 72-74, (November 13, 1995).

How To Protect Yourself From the Credit Fraud Epidemic, in Your Money Monitor, Perry, Nancy J., Money Magazine, pp. 38-42, (August 1995).

Invasion of the Credit Snatchers by McMenamin, Brigid, Forbes, pp. 256-259, (August 26, 1996). The latest credit card fraud involves thieves who tap into files at a credit reporting agency and steal the identity of people with good credit ratings.

Mail Order Madness by Deborrah M. Wilkinson. Black Enterprise, pp. 123-127, (July 1996). Gives tips on how to evaluate the offerings in your e-mail with shopper "dos and don'ts."

New Generation of High-Tech Scams, Consumers Research, pp.19-21, (March 1996).

Safety Net: Does Using The Internet Put Your Business At Risk? By Cheryl J. Goldberg. Entrepreneur, pp. 48-50, (September 1996). Doing business on the Internet offers opportunity for crimes, such as spreading of viruses, credit card number theft and theft of intellectual property. Tips are given on how to make online usage more secure.

Self-Interest and Consumers by Frances B. Smith. Consumers' Research Magazine, pp. 33-37, (April 1996). The media and many consumers do not understand that protecting consumers from fraudulent companies is in the best interest of the competitors.

Shopping Online: What You Need To Know by Roberta Furger. PC World, pp. 320-322, (June 1996). Online shopping is not risk-free, however, users need not avoid it altogether if they take simple precautions and keep certain facts in mind. Also includes the Federal Trade Commission precautions.

Sign Here, Please. Consumer Reports, p. 87, (April 1996). Discusses credit card digital signature devices.

The Eight Biggest Rip-Offs in America.... And How You Can Avoid Being A Victim by Shelly Branch, Lani Luciano, Teresa Tritch, Amanda Walman and Ruth Simon. Money Magazine, pp. 142-148, (August 1995). Some of the most egregious common consumer traps.

The Wild, Wild Web by Gregory Spears. Kiplinger's Personal Finance Magazine, pp. 59-68, (November, 1996). Online investing tips and information on fraud in online investing.

You Don't Have To Fret About Using A Credit Card On The Net by Duff McDonald. Money Magazine, p. 45, (October 1996). Fears about credit card fraud occurring on the Internet are greatly exaggerated.

Pamphlets

The Department of Financial Institutions has brochures available on their Web Site: http://www.dfi.state.in.us/uccc/Lists/LIST%20CREDIT%20BROCHURES.html

Cybershopping: Protecting Yourself When Buying Online
Investment Swindles: How They Work and How To Avoid Them
Online Scams: Potholes on the Information Highway
Swindlers Are Calling

Available for $.50 each from
R. Woods
Consumer Information Center
Pueblo, CO 81009

Business Opportunity Scams: Vending machines and Display Racks
Car Financing Scams
Credit and Charge Card Fraud
Credit Repair: Self-Help May Be Best
Easy Credit? Not So Fast: The Truth About Advance-Fee Loan Scams
"800" and International Telephone Number Scams
Fraudulent Health Claims: Don't Be Fooled
Modeling Agency Scams
Prize Offers
Telecommunications Scams Using FCC Licenses
Telemarketing Recovery Scams
Telemarketing: Reloading and Double-Scamming Frauds
Telemarketing Travel Fraud
Wealth-Building Scams

Available free from:
Public Reference, Room 130
Federal Trade Commission at http://www.ftc.gov
Washington, DC 20580-0001

Fax: 202-326-2572
Internet: http://www.ftc.gov

Schemes, Scams & Flim-Flams

Available free from:
MasterCard
Telephone: 1-800-999-5136

Internet

The following resources provide information on fraud and list the current scams on the Internet.

Indiana Department of Financial Institutions other Web Sites on Fraud at http://www.dfi.state.in.us/uccc/end.htm#fh

Better Business Bureau at http://www.bbbonline.org

Consumer World at http://www.consumerworld.org

National Fraud Information Center at http://www.fraud.org
Telephone: 1-800-876-7060

Securities and Exchange Commission at http://www.sec.gov/consumer/cyberfr.htm

Webmaster at http://www.consumer.com

SWINDLERS HAVE COMPUTERS TOO

Cyberspace is a vast new territory for unscrupulous marketers. The National Fraud Information Center reports that while fraudulent commercial activity on the Internet is not yet a major problem, as use expands, there is sure to be a major increase in deceptive and misleading promotions.

Swindlers are attracted to the Internet because they can reach thousands of consumers inexpensively, quickly and anonymously. Few restrictions exist on the Internet, making it easy to place deceptive or misleading information online.

Judging the accuracy and reliability of online information is a major challenge for consumers. False or misleading information related to personal finance or health issues, for example, could lead to serious consequences for unsuspecting consumers.

FRAUD ON THE NET

The Federal Trade Commission began investigating fraud on the Internet in 1994. They found that the same kinds of fraud that occur in other places also surface on the Net. Electronic bulletin boards, chat groups, and e-mail networks are fertile grounds for old-fashioned scams that apply false advertising claims and deceptive marketing practices.

Electronic Bulletin Boards provide new sources of information to Internet users telling about products, services, and investment opportunities. At the same time these electronic bulletin boards can carry false and misleading ads for products that promise quick solutions to desirable goals such as weight loss or easy business success. The plan is to have you use your PC to make plenty of money in a short period of time.

Discussion groups or chat forums often form on the Internet where interested parties can exchange information on specific topic areas. These chat rooms sometimes appear to be open discussion when they are sales pitches in disguise. In some cases, people involved in the discussion may have financial ties to businesses that sell products or services related to the topic area. This disguised advertising may not be obvious to the consumer.

E-mail scams involve individuals or companies intentionally misleading consumers or using deceptive marketing practices to gain the consumer's interest in their product. For example, the use of a particular product is advertised to cure a specific medical condition. These are the same health, diet, and fitness schemes that occur in other marketplace venues, such as mail-order and telemarketing schemes. Other types of e-mail scams involve the sale of worthless products, phony credit repair companies, term paper peddlers, expensive work-at-home deals, psychic hotlines, and deceptive promises related to contests, awards, sweepstakes, and free gifts.

Pyramid or Ponzi schemes and chain letters are well suited to the Internet because they entice investors with the promise of quick profits using a home computer. Investors make money by recruiting new investors. The problem is that soon the program runs out of new investors and most players lose the money they invested. Chain letter schemes ask participants to send money to the names at the top of a list with the promise that they will eventually receive thousands of dollars when their names come to the top. Unsuspecting persons lose money every day on this illegal practice.

Risk-free investment opportunities on the Internet offer fraudulent technological and exotic investments such as wireless cable, bogus securities, or worthless land. These investments promise to yield far greater returns than do commonly available investment products. The term "risk-free" is highly misleading. Few consumers get their money back, much less make a profit.

Pump and Dump stock manipulations on the Internet encourage investors to buy a particular stock, which is usually little known and low cost. The promoters may even advertise that they have inside information. They make their profit when consumers buy the stock, or pump up the price and the promoters then promptly sell, or dump their shares and the stock prices immediately fall. This scheme can also work in reverse; a short seller makes a profit when the price of the stock goes down.

PROBLEMS WITH INTERNET TRANSACTIONS

Two problems with Internet sales transactions are personal data privacy and verification that both buyers and sellers are authentic. Many consumers are concerned about the confidentiality of their personal financial information on the Web, with good reason. When you make a purchase on the Internet, your credit card number could fall into the wrong hands. Personal data can be collected and organized into database files. When you become a part of an on-line service, your personal data can be available to everyone in that system. While it is unlikely that reputable merchants would deliberately sell your data to others, their database may be tempting targets for hackers.

Verification that consumers are who they say they are can be solved by an electronic equivalent of a signature or a driver's license. A software product currently used by merchants, banks, and brokerage houses tells who the user is and what privileges he or she has. There is a growing interest in credit card payment systems that would safeguard credit card purchases on the Net. Encryption software can scramble your personal information so that it can be read only by the sender and the receiver. The problem remains that personal data might still be available to certain employees or hackers.

Experts urge consumers to avoid dealing with Internet sites they are not familiar with. Even when dealing with a well-known business, call the business directly to verify that the site exists. It continues to be a risky business to give personal information, including address and phone number, credit card numbers, social security numbers, and bank account numbers on the Internet.

PROTECTION AGAINST INTERNET FRAUD

Most people find it hard to believe that they could become victims of fraud, but one should never underestimate the ingenuity of swindlers who make money by misleading others. State and federal laws and agencies have limited capacity to protect consumers from fraud on the Internet. The savvy consumer must stay alert to the possibility of fraud. The National Fraud Information Center offers the following suggestions for side-stepping fraud on the Internet:

Never reveal checking account numbers, credit card numbers, or other personal financial data at any Web site or online service location -- unless you are sure you know where this information will be directed.

When you subscribe to an on-line service you may be asked for credit card information. When you enter any interactive service site however, beware of con artists who may ask you to "confirm" your enrollment in the service by disclosing passwords or the credit card account number used to subscribe.

Use the same common sense you would exercise with any direct or telephone credit card purchase. A flashy professional Internet Web site does not guarantee that the

sponsor is legitimate. Know the company with which you plan to do business.

Report anything you see on the Internet that you suspect might be fraudulent. The National Fraud Information Center's toll-free number is 1-800-876-7060. Their mailing address is P.O. Box 65868, Washington, D.C. 20035. Their Web address is http://www.fraud.org

Your state Office of the Attorney General is empowered to investigate consumer complaints, including Internet complaints. They can give you information about any problems or concerns they have encountered with the business.

The Better Business Bureau can tell you if there have been any complaints or inquiries about a business and how it was resolved. Some online advertisements will have a blue-seal that you can click on to connect to the Better Business Bureau for a report on the advertiser's track record. The online Web site for the BBB is http://www.bbbonline.org

The Federal Trade Commission enforces several consumer protection laws that are relevant to computer transactions, such as false advertising and consumer credit. Suspicious actions on the Web, when reported to the National Fraud Information Center, are shared with the Federal Trade Commission and the National Association of Attorneys General. In this way, consumers join with state and federal agencies in actions to curtail fraud on the Internet.

Although many regulations and agencies have been established to protect consumers from fraud, the principle of let the buyer beware remains the consumer's best protection. Legal protections are limited, fraudulent activities flourish, and once money is lost in a fraudulent scheme the chances of getting it back are extremely small. Awareness of the possibility of fraud is your first line of defense.

The Indiana Department of Financial Institutions, Division of Consumer Credit has many other credit related brochures available. Call our toll-free number or write to the address on the cover for a copy of any of our listed or for further consumer credit information. You can also access information at our web site on the Internet: http://www.dfi.state.in.us, then click on Consumer Credit.

FRAUD ON THE INTERNET

DEPARTMENT OF FINANCIAL INSTITUTIONS
Consumer Credit Division
402 West Washington Street, Room W066
Indianapolis, Indiana 46204
317-232-3955
1-800-382-4880
Web Site http://www.dfi.state.in.us